

AI+ Security Strategist

OEM: AI CERTs • Duration: 5 Days (40 hrs) • Code: AT-2103

COURSE MODULES & TOPICS

At a Glance: Course + Exam Overview

- Instructor-Led: 5 days (live or virtual)
- Self-Paced: 40 hours of content

Who Should Enroll?

- Cybersecurity Professionals: Individuals looking to enhance their skills in compliance and security management.
- Risk Management Specialists: Those interested in improving risk assessment and mitigation strategies using AI.
- Compliance Officers: Professionals responsible for ensuring adherence to regulatory standards who want to leverage AI for compliance processes.
- IT Security Analysts: Analysts seeking to integrate AI technologies into their security practices and frameworks.
- Ethical Hackers and Penetration Testers: Individuals wanting to explore AI techniques for identifying vulnerabilities, defending against adversarial attacks, and stress-testing systems.
- Tech-Savvy Leaders: IT managers or security architects aiming to future-proof their organizations with AI-enhanced compliance, governance, and security practices.
- Aspiring AI Security Experts: Learners with foundational knowledge in AI and cybersecurity eager to master AI-powered solutions for emerging threats and advanced security challenges.

Skills You'll Gain

- AI-driven cybersecurity strategy and risk management
- Designing AI-powered security frameworks and defense strategies
- Security governance, compliance, and responsible AI practices
- AI threat modeling and cybersecurity risk assessment
- Evaluating AI security tools and technologies
- Developing organizational AI security adoption strategies
- Managing AI-related risks, policies, and controls
- Integrating AI into enterprise security operations
- Building secure and resilient AI-driven environments
- Making strategic cybersecurity decisions using AI insights

What You'll Learn

- This module focuses on automating role-based access controls, detecting unauthorized access, and implementing AI-driven MFA systems. You'll also explore real-world applications of reinforcement learning and AI-based fraud detection in IAM scenarios.
- This module covers AI solutions for securing smart cities, industrial IoT, and autonomous vehicles. You'll also learn about federated learning for decentralized security and techniques for safeguarding smart home devices against unauthorized access.
- This module guides you through every step, from defining project goals and selecting datasets to integrating AI models into existing infrastructures. You'll gain hands-on expertise in creating scalable, adaptive, and effective security solutions.

Prerequisites

- Foundation in AI+ Security : Completion of AI+ Security Compliance Practitioner and AI+ Security Practitioner.
- Intermediate / Advanced Python Programming : Proficiency in Python, including experience with deep learning tools like TensorFlow and PyTorch.
- Advanced Cybersecurity Knowledge : Strong skills in threat detection, incident response, and securing networks and devices.
- Cloud and Blockchain Basics : Understanding of cloud security, container systems, and blockchain technology.
- Linux/CLI Mastery : Advanced command-line skills and experience with security tools in Linux environments.
- AI in Security Engineering : Knowledge of AI's role in identity and access management (IAM), IoT security, and physical security.

Exam Blueprint:

- Foundations of AI and Machine Learning for Security Engineering - 5%
- Machine Learning for Threat Detection and Response - 5%
- Deep Learning for Security Applications - 5%
- Adversarial AI in Security - 6%
- AI in Network Security - 6%
- AI in Endpoint Security - 8%
- Secure AI System Engineering - 8%
- AI for Cloud and Container Security - 11%
- AI and Blockchain for Security - 11%
- AI in Identity and Access Management (IAM) - 12%
- AI for Physical and IoT Security - 12%
- Capstone Project - Engineering AI Security Systems - 11%

Choose the Format That Fits Your Schedule

- High-Quality Videos, E-book (PDF & Audio), and Podcasts
- AI Mentor for Personalized Guidance
- Quizzes, Assessments, and Course Resources
- Online Proctored Exam with One Free Retake
- Comprehensive Exam Study Guide
- 5 days of intensive training with live demos
- Real-time Q&A, peer collaboration, and hands-on labs
- Led by AI Certified Trainers and delivered through Authorized Training Partners

- ~40 hours of on-demand video lessons, e-book, podcasts, and interactive labs
- Learn anywhere, anytime, with modular quizzes to track progress